



# CRYPTO: IS IT TOO MUCH PROTECTION?

**Walker W. Watson**

October, 6, 1993

# **Risk Exposure**

**When 25-80 percent of a firm's cash flow is on line, technology risk becomes business risk.**

**Many business managers are unaware of the range of IT-related risks to which a firm is exposed.**

**They learn about most of them only through disaster.**

# **Major Risks**

**Two major areas of exposure are:**

- **Security**

**a growing problem in terms of  
vulnerability to criminal theft and  
fraud and accidents of leakage  
information.**

- **Network Management**

**involves a different form of risk that  
requires a highly complex technical  
infrastructure to protect the firm.**

# **Computer Crime**

**A 1986 survey of 100 accountants and 90 mid-level Information Technology professionals at a conference on computer security found that three-quarters believed that most electronic thieves are caught by accident.**

## **Quotation**

**“ This [the un-detection of electronic thieves] is a startling admission of the vulnerability of the accounting controls, audit trails and programming documentation for which their professionals [accountants, and IT managers] are responsible. ”**

# **Criminal Activity**

**No one knows the true level of computer crimes-successfull crimes may avoid detection entirely-**

**study of those detected finds they involved far greater sums of money than other white collar crimes.**

# Hackers & Crackers

## ■ Hackers

- computer pioneer
- sixties generation
- became rich, got authority

## ■ Crackers

- new generation
- alienated
- digital criminals



# Information

- **Information can't be stolen**
  - **property laws for tangible objects**
  - **raw data**
  - **ownership obsolete**
- **Information can be copied**
  - **perfect copy**
  - **original intact**



# **Money and Computer Crime**

## **■ Richard Nixon**

- removed gold standard**
- money became bits and bytes**
- stopped using reality as "acid test"**

## **■ Society is digital**

- easy to change**
- good programmer: no fingerprints**

# **Cracking the Bank**

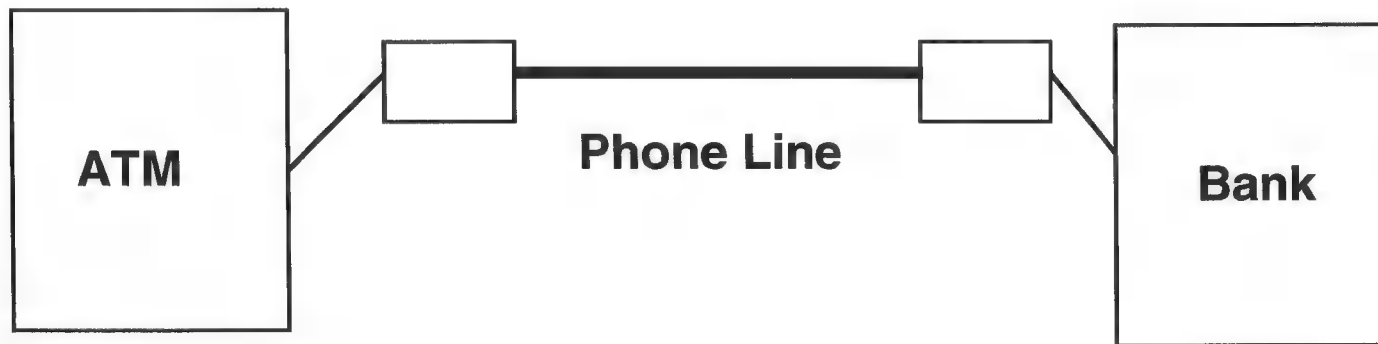
## **■ ATM (Automated Teller Machines)**

- all banks use them**
- security nonchalant**
- vulnerable system**

## **■ On-Site vs Off Site**

- On-Site protected**
- Off-Site convenience no protection**

# ATM Data Path



- **Customer uses card and PIN**
- **Data transmit over phone**
- **Banks OKs transaction**
- **Banks send authorization over phone**

# ATM Exposure

- Phone lines unprotected
- No encryption of data over phone lines
- Gas stations and grocery stores easy targets
- Personal account information vulnerable
- Inside protection, but none outside
- Losses covered to avoid bad publicity
- Court transcripts/newspaper accounts provide necessary information to criminals

# Safe Communications

**“ Telecommunications security is a source of increasing concern for individuals, corporations, and governments. As the flow of information increases, so does the likelihood of exposure to wrong parties. ”**

# **Race is ON**

- **Worldwide competition heating up**
- **Traditional spies turn to industrial espionage**
- **60% daily business communications over telephone lines**
- **Much information is sensitive and propriety**

# **CLIPPER CHIP**

- **Data Encryption for business**
- **Hardware device**
- **Government sponsored development**
- **Government endorsed**
- **Law Enforcement support**
- **Constitutional questions**



# Who Holds the Keys?

- Two keys for encryption and decryption
- Government holds one
- Private firm holds other
- Algorithm is classified **SECRET**
- Are they secure?
- Subject to Government leaks?
- Is it accepted by public?

# **Constitutional Questions**

- **Can we trust the Government?**
- **Will criminals register?**
- **Are privacy rights violated?**
- **Will Clipper become law?**
- **Is Clipper best technology?**
- **Can government administer?**
- **Does it stop here?**